Introduction to Ethical Hacking

By Carla A. Varela Rosa
“Hacking involves a different and creative way of looking at problems in ways that no one has thought of.”

- Someone Famous
The hacker

Regardless of their motivation, a hacker is a person that uses tools, techniques, knowledge, and skills to circumvent system security measures to gain access to information or hack the system.
The Motivation of the Hacker

- Show Off
- Protect and defend
- $$$$
- Acquire new skills
- Be challenged
Profile of a Hacker

*The Hat System*

- **Black hat**: The Bad
- **Grey hat**: The Undecided
- **White hat**: The Good
**Other**

**Script kiddies**
- Person that lacks technical skills, sociability and even maturity.
- Person who claims to have knowledge or skills that he does not have.
- It describes people who use programs and scripts developed by others to attack computer systems and networks.

**Hacktivistas**
- They do harm to computer systems or a network for social or political reasons.
- Hacktivism seeks to draw the public’s attention to an particular issue.
- They are usually not looking to hurt but to leave a visible message.

**Phreaker**
- Phone + Hacker
- They are basically a telecommunication hacker.
Why do we need the Ethical Hacker?
Is it legal?

- It is completely legal as long as it is done with the **proper authorization** of the administrators and owners of the systems.
Is it legal?

- The best way to guarantee that something is safe is to carry out a **fictitious attack**, that’s why we need ethical hackers.
Is it legal?

Ethical hackers must have:

- specific limits
- contracts
- nondisclosure agreement
- confidentiality agreement
- start and end date
THINK LIKE THE ENEMY
**Stages**

01 Reconnaissance
   - Information gathering.
   - active/passive

02 Scanning and Enumeration
   - We begin to ‘touch’ the system.

03 Gaining Access
   - Using methods to bypass security.

04 Maintaining Access
   - Using methods to stay in the system as long as possible.

05 Covering tracks
   - Avoid being detected.
**Reconnaissance**

Information gathering phase!

**Active**
We directly interact with the target to gather information.
Most common tools used: nmap

**Passive**
We try to collect information about the target without directly interacting or accessing it.

Common strategies:
- collecting information from social media
- collecting information from public websites
[2] SCANNING AND ENUMERATION

Perform scans to enumerate elements in target. Some strategies include:

- Port Scanning
- Vulnerability Scanning
- Network Mapping
We want to collect enough information to gain access to the target. Strategies used:

- password cracking
  - online
  - offline
- password guessing
- rainbow tables
- dictionary attacks
[4] MAINTAINING ACCESS

At this stage we take steps to secure our presence. Some strategies include:
- the use backdoors [Trojan]
- Rootkits

[5] COVERING TRACKS

At this stage we want to avoid being detected! Some strategies include:
- deleting or changing logs
- delete all documents and files created
THE PENTEST

It is an attack on a computer system with the intention of finding security weaknesses or attack vectors that lead to data leakage of a door for any type of attack.

The ethical hacker knows all the details of the target of evaluation including infrastructure and passwords.

The ethical hacker knows certain information about the target of evaluation.

The ethical hacker knows nothing about the target of evaluation.
Preparation and Certifications

- **CEH**: Certified Ethical Hacking Certification
- **GPEN**: GIAC Penetration Tester
- **OSCP**: Offensive Security Certified Professional
- **CREST**: Highly recognized.
Thank You!